

WHAT IS CLAIMED IS:

1 1. A method processing one or more files using a security application, the
2 method comprising:
3 connecting the client to a proxy server, the proxy server being coupled to one
4 or more NAS servers;
5 requesting for a file from a client to the proxy server;
6 authenticating a requesting user of the client;
7 authorizing the requesting user for the file requested;
8 requesting for the file from the one or more NAS servers after authenticating
9 and authorizing;
10 requesting for the file from the one or more storage elements;
11 transferring the file from the one or more storage elements through the NAS
12 server to the proxy server;
13 determining header information on the file at the proxy server;
14 identifying a policy based upon the header information at the proxy server;
15 processing the file according to the policy, the processing including
16 decompressing the file, decrypting the file, and verifying the file; and
17 transferring the processed file to the user of the client.

1 2. The method of claim 1 wherein the file comprises retrieval and
2 verification information.

1 3. The method of claim 1 wherein the decryption is provided by a NIST
2 approved process.

1 4. The method of claim 1 wherein the NIST approved process is selected
2 from AES and Triple-DES.

1 5. The method of claim 1 wherein the verifying comprises processing a
2 keyed message authentication code.

1 6. The method of claim 5 wherein the keyed message authentication code
2 is generated using a SHA-1 or MD-5 or SHA-512.

1 7. The method of claim 1 further comprising determining one or more
2 statistics in a database on a security device.

1 8. The method of claim 7 wherein the database is a secure catalog
2 database.

1 9. The method of claim 8 further comprising using the secure catalog
2 database to detect an intrusion.

1 10. The method of claim 1 further comprising adding information
2 associated to positional integrity to the file.

1 11. The method of claim 1 further comprising generating a signature
2 record on the file to detect any modification of the file.

1 12. The method of claim 1 further comprising identifying a number of
2 blocks stored within a database, the database including the file.

1 13. A system for providing security on a network attached storage, the
2 system comprising:

3 a directed proxy server coupled to a databus, the databus being coupled to a
4 plurality of clients, the directed proxy server being adapted to add header information and to
5 add trailer information on a file by file basis, the directed proxy server being adapted to
6 provide policy information on either or both the header information and the trailer
7 information;

8 a NAS server coupled to the directed proxy server; and
9 one or more storage device coupled to the filer.

1 14. The system of claim 13 wherein the directed proxy server
2 communicates to the filer using an access protocol selected from NFS or CIFS format.

1 15. The system of claim 13 wherein the directed proxy sever is transparent
2 to a user.

1 16. The system of claim 13 wherein the NAS server is transparent to the
2 plurality of clients.

1 17. The system of claim 13 wherein the directed proxy server operates at a
2 wire speed to add header information and trailer information.

1 18. The system of claim 13 wherein the directed proxy server is adapted to
2 maintain a plurality of security keys, one or more of the keys is associated with a group of the
3 files.

1 19. The system of claim 13 wherein the directed proxy server is adapted to
2 maintain a plurality of security keys, one or more of the keys is associated with a user.

1 20. The system of claim 13 wherein the policy information is associated
2 with a service, the service is selected from an encryption process, a decryption process, an
3 authentication process, an integrity process, a compliance process, an intrusion detection
4 process, or a promotion process.

1 21. A method processing one or more files using a security application, the
2 method comprising:

3 connecting a security device to a NAS server, the NAS server being coupled to
4 one or more storage elements;

5 detecting one or more changed files on the NAS server;

6 detecting one or more portions of the one or more files that have been
7 changed;

8 determining a policy information for at least one of the changed files to
9 determine a security attribute information;

10 generating header information for the changed file;

11 attaching the header information on the changed file;

12 processing at least one portion of the changed file according to the policy
13 information, the processing including:

14 compressing the portion;

15 encrypting the portion;

16 generating one or more message authentication codes associated with the
17 portion of the changed file;

18 transferring the changed file to one or more of the storage elements.

1 22. The method of claim 21 wherein the processing is provided at wire
2 speed.

1 23. The method of claim 21 wherein the one or more of the storage
2 elements is a storage area network.

1 24. The method of claim 21 wherein the transferring of the changed file is
2 provided via SCSI interface.

1 25. The method of claim 21 wherein the policy information is provided in
2 a library.

1 26. The method of claim 21 wherein the encrypting is decrypting.

1 27. A method processing one or more files using a security application, the
2 method comprising:

3 connecting the client to proxy server, the proxy server being coupled to one or
4 more NAS servers;

5 transferring a file from a client to the proxy server;

6 authenticating a user of the client;

7 authorizing the user for the file requested;

8 processing the file using a keyed message authentication integrity process;

9 generating header information for the file;

10 attaching the header information on the file;

11 transferring the file to one or more of the NAS servers;

12 transferring the file from the one or more NAS servers to one or more storage
13 elements.

1 28. The method of claim 27 further comprising encrypting the file using a
2 key size of at least 128 bits to form an encrypted file.

1 29. The method of claim 28 wherein the encrypting is provided using a
2 NIST approved process.

1 30. The method of claim 28 wherein the encrypting is provided using
2 AES-128, AES-192, AES-256, Triple-DES.

1 31. The method of claim 27 wherein the keyed message authentication
2 integrity process is provided by SHA-1, SHA-2, MD-5.

1 32. The method of claim 27 wherein the processing is provided at
2 wirespeed, the wirespeed being greater than 1 Gigabit/second.

1 33. The method of claim 27 wherein the authenticating, authorizing,
2 processing, generating, and attaching are provided at the proxy server.

1 34. The method of claim 27 wherein the header information comprises at
2 least one element selected from a time stamp, Encrypted Data Encrypted Key, Encrypted
3 Data Hash MAC key, and File attributes.

1 35. The method of claim 27 further comprising transferring the file to one
2 or more to other storage elements.

1 36. A method processing one or more files using a security application, the
2 method comprising:
3 connecting the client to server, the server being coupled to one or more storage
4 elements;
5 transferring a file from a client to the server;
6 authenticating a user of the client;
7 authorizing the user for the file requested;
8 processing the file using a keyed message authentication integrity process;
9 generating header information for the file;
10 attaching the header information on the file; and
11 transferring the file to one or more of the storage elements.

1 37. The method of claim 36 further wherein the one or more storage
2 elements comprises one or more NAS servers to one or more storage elements.

1 38. The method of claim 36 further comprising encrypting the file using a
2 key size of at least 128 bits to form an encrypted file.

1 39. The method of claim 38 wherein the encrypting is provided using a
2 NIST approved process.

1 40. The method of claim 38 wherein the encrypting is provided using
2 AES-128, AES-192, AES-256 or Triple-DES.

1 41. The method of claim 36 wherein the keyed message authentication
2 integrity process is provided by SHA-1, SHA-2, MD-5.

1 42. The method of claim 36 wherein the processing is provided at
2 wirespeed, the wirespeed being greater than 1 Gigabit/second.

1 43. The method of claim 36 wherein the authenticating, authorizing,
2 processing, generating, and attaching are provided at the proxy server.

1 44. The method of claim 36 wherein the header information comprises at
2 least one element selected from a time stamp, Encrypted Data Encrypted Key, Encrypted
3 Data Hash MAC key, and File attributes.

1 45. A method for providing secured storage of data, the method
2 comprising:
3 providing a key encryption key;
4 storing the key encryption key on a system;
5 storing a message authentication code generating key on the system;
6 decrypting a file encryption key with the key encryption key;
7 decryption a file message authentication code generating key with the key
8 encryption key;
9 using the file encryption key to decrypt data stored on a server or encrypt data
10 originated by a user on a client;
11 generating a message authentication code for a header of the file with the
12 message authentication code generating key; and
13 using the file message authentication code generating key to generate one or
14 more message authentication codes block by block in the file.

1 46. The method of claim 45 wherein the file encryption key is provided in
2 the file.

1 47. The method of claim 45 wherein the file message authentication key is
2 provided in the file.

1 48. The method of claim 45 wherein the file message authentication key
2 verifies content of data of the file upon a read process.